CHAPTER

19

Viruses, Disaster Recovery, and a Maintenance Plan That Works

In this chapter, you will learn:

- About preventive maintenance and procedures designed to protect systems
- How to develop a preventive maintenance plan
- How systems become infected with viruses and other infestations
- How viruses work, how to protect systems against them, and how to deal with them when they infect your system
- About the strengths and weaknesses of different backup procedures and systems, and how to use backup software
- How to develop a disaster recovery plan

When you are responsible for a computer, regular maintenance can help prevent disaster, lower repair costs, and make problems less disruptive. Two important tasks in preventive maintenance are making regular backups of hard drives and dealing with viruses. These two tasks, as well as routine hardware maintenance and designing a disaster recovery plan, are addressed in detail in this chapter.

PREVENTIVE MAINTENANCE

If you are responsible for the PCs of an organization, make and implement a preventive maintenance plan to help prevent failures and reduce repair costs and downtime. In addition, you need a disaster recovery plan to manage failures when they occur. PC failures are caused by many different environmental and human factors, including heat, dust, magnetism, power supply problems, static electricity, human error (such as spilled liquids or an accidental change of setup and software configurations), and viruses. The goals of preventive maintenance are to reduce the likelihood that the events that cause PC failures will occur and to lessen the damage if they do occur. When designing a preventive maintenance plan, consider what you can do to help prevent each cause, and write into the plan the preventive actions you can take. Think through the situation caused by each problem. What would happen to the PC, the software, the data, the user's productivity, and so on, if a failure occurred? What would you do and what materials would you like to have in that situation? What can you do ahead of time to help make the situation less disastrous? Your answers to those questions will lead you to create effective preventive maintenance and disaster recovery plans. This section focuses on the preventive maintenance plan.

For example, consider the problem caused by a user accidentally changing CMOS setup. What can you do to prevent that from occurring? If it does occur, how can you solve the problem? What can you do now to prepare for that event? By answering these three questions, you might arrive at these preventive maintenance and recovery procedures: (1) make a backup copy of setup to floppy disk, (2) label the disk and keep it in a safe place, (3) educate the user about the importance of not changing setup, and (4) keep a maintenance record of this PC, including the last time setup was backed up.

A Preventive Maintenance Plan

If your company has established written guidelines for PC preventive maintenance, read them and follow the necessary procedures to make them work. If your company does not have an established plan, make your own. A preventive maintenance plan tends to evolve from a history or pattern of malfunctions within the organization. For example, dusty environments can mean more maintenance, whereas a clean environment can mean less maintenance. Table 19-1 lists some guidelines for developing a preventive maintenance plan that may work for you.

A+ CORE 3.1

TIP

Dust is not good for a PC because it acts like a blanket, insulating PC parts, which can cause them to overheat; therefore, ridding the PC of dust is an important part of preventive maintenance. Some PC technicians don't like to use a vacuum inside a PC because they're concerned about ESD that the vacuum might produce. Use compressed air to blow the dust out of the chassis, power supply and fan, or use a special anti-static vacuum designed to be used around sensitive electronic equipment.

A+CORE 3.1, 5.2

Table 19-1 Guidelines for developing a PC preventive maintenance plan

Component	Maintenance	How Often
Inside the case	■ Make sure air vents are clear. ■ Use compressed air to blow the dust out of the case, or use a vacuum to clean vents, power supply, and fan. ■ Ensure that chips and expansion cards are firmly seated. ■ Clean the contacts on expansion cards.	Yearly
CMOS setup	Keep a backup record of setup (for example, use Nuts & Bolts rescue disk).	Whenever changes are made
Floppy drive	Only clean the floppy drive head when the drive does not work.	When the drive fails
Hard drive	■ Perform regular backups. ■ Automatically execute a virus scan program at startup. ■ Defragment the drive and recover lost clusters regularly. ■ Don't allow smoking around the PC. ■ Place the PC where it will not be jarred, kicked, or bumped.	At least weekly At least daily Monthly Always Always
Keyboard	■ Keep the keyboard clean. ■ Keep the keyboard away from liquids.	Monthly Always
Mouse	■ Clean the mouse rollers and ball (see Chapter 8).	Monthly
Monitor	■ Clean the screen with a soft cloth.	At least monthly
Printers	■ Clean out the dust and bits of paper, using compressed air or a vacuum. Small pieces of paper can be removed with tweezers. ■ Clean the paper and ribbon paths with a soft lint-free cloth. ■ Don't re-ink ribbons or use recharged toner cartridges. ■ If the printer uses an ozone filter, replace it as recommended by the manufacturer.	At least monthly or as recommended by the manufacturer
Software	■ If directed by your employer, check that only authorized software is present. ■ Regularly delete files from the recycle bin and \Temp directories. ■ Delete any temporary files in the \DOS directory.	At least monthly
Written record	■ Keep a record of all software, including version numbers and the OS installed on the PC. ■ Keep a record of all hardware components installed, including hardware settings. ■ Record when and what preventive maintenance is performed. ■ Record any repairs done to the PC.	Whenever changes are made

A+ CORE 3.1

The general idea of preventive maintenance is to do what you can to make a PC last longer and give as little trouble as possible. You may also be responsible for ensuring that data is secure and backed up, that software copyrights are not violated, and that users are supported. As with any plan, when designing your preventive maintenance plan, first define your overall goals, and then design the plan accordingly. The guidelines listed in Table 19-1 address primarily the problems that prevent a PC from lasting and from performing well.

Recordkeeping and protecting software and hardware documentation are often overlooked during preventive maintenance. A record of what is done to a PC is valuable when solving problems or considering an upgrade. Secure all manufacturer hardware documentation, such as for a sound card or modem, to prevent accidental loss or destruction. You can file these documents in an envelope with a log of everything you have done to the PC for regular maintenance, installations, and repairs. Be sure to include a boot disk that contains a copy of CMOS setup for this PC. Consider taping the envelope to the inside of the computer case, especially when you are responsible for PCs at off-site locations where you might not have assigned filing cabinet space. You can also keep this information in a notebook along with other similar notebooks at your workstation. Label each notebook to identify the PC that it tracks. You can also keep records on a separate PC.

Tidy the hard drive after installing an OS or an application. For example, after installing Windows 9x, delete temporary files from the \DOS directory and from the \Windows\Temp directory. Also, when you initially set up a PC, if you are using an older version of DOS, check the SET TEMP command in the AUTOEXEC.BAT file. If it reads SET TEMP=C:\DOS, change it to SET TEMP=C:\TEMP and create a \TEMP directory. Storing temporary files in the \DOS directory can create problems. In addition to the list in Table 19-1, encourage users to follow routine steps as part of your preventive maintenance plan. For instance, ask a user to conserve hard drive space by regularly deleting the files in the \TEMP or \Windows\Temp directory. For Windows 9x, Windows NT, and Windows 2000, regularly empty the Recycle Bin by deleting its files. Routinely back up the hard drive (for a more efficient backup process, you can back up only directories that contain data). You will learn more about hard drive backups later in the chapter. Ask the user not to block the air vents on the back of the monitor or computer case and not to place the case on the floor where it can be kicked.

When Moving Equipment

When shipping a PC, rough handling can cause damage, as can exposure to water, heat, and cold. The PC can also be misplaced, lost, or stolen. When you are preparing a PC for shipping, take extra precautions to protect it and its data. Follow these general guidelines when preparing to ship a PC:

- Back up the hard drive onto a tape cartridge. If you don't have access to a tape cartridge, back up important system and configuration files to a floppy disk. Whatever you do, don't ship a PC that has the only copy of important data on the hard drive or data that should be secured from unauthorized access.

- Remove any floppy disks, tape cartridges, or CDs from the drives. Make sure that the tapes or disks holding the backup data are secured and protected during transit. Consider shipping them separately.
- Turn off power to the PC and all other devices.
- Disconnect power cords from the electrical outlet and the devices. Disconnect all external devices from the computer.
- If you think someone might have trouble later identifying which cord or cable belongs to which device or connection, label the cable connections with white tape or white labels.
- Coil all cords and secure them with plastic ties or rubber bands.
- Pack the computer, monitor, and all devices in their original shipping cartons or similar boxes with enough packing material to protect them.

Disposing of Used Equipment

A+CORE 3.2

As a PC technician, it will often be your responsibility to dispose of used equipment and consumables, including batteries, printer toner cartridges, and monitors. Table 19-2 lists items and how to dispose of them. Manufacturer documentation and local environmental regulators can also provide disposal instructions or guidance. Monitors and power supplies can contain a charge even after the devices are unplugged. To discharge the capacitors in either device, place a screwdriver across a hot prong and the ground prong of the electrical connections as shown in Figure 19-1. To discharge the actual CRT in a monitor, the monitor must be opened. Ask a technician trained to fix monitors to do this for you.

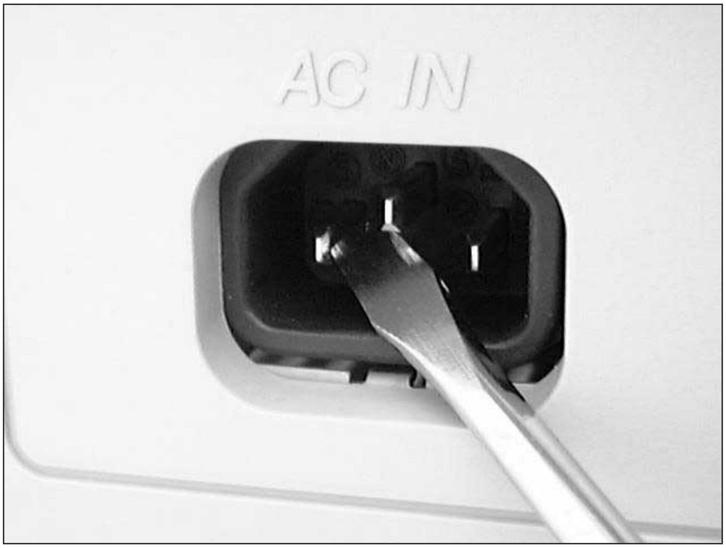


Figure 19-1 Discharge the capacitors in a monitor before disposal

A+CORE 3.2

A **material safety data sheet (MSDS)** explains how to properly handle substances such as chemical solvents. An MSDS includes information such as physical data, toxicity, health effects, first aid, storage, disposal, and spill procedures. It comes packaged with the chemical, or you can order one from the manufacturer, or find one on the Internet (see *www.ilpi.com/msds)*.

Table 19-2 Computer parts and how to dispose of them

Part	How to Dispose
• Alkaline batteries including AAA, AA, A, C, D, and 9 volt	Normal trash
• Button batteries used in digital cameras, Flash Path, and other small equipment • Battery packs used in notebooks	These batteries can contain silver oxide, mercury, lithium, or cadmium and are considered hazardous waste. Dispose of these either by returning them to the original dealer or taking them to a recycling center. To recycle them, pack them separately from other items. If you don't have a recycling center nearby, contact your county for local regulations for disposal.
• Laser printer toner cartridges	Return to the manufacturer or dealer to be recycled
• Ink-jet printer ink cartridges • Computers • Monitors • Chemical solvents and cans	Check with local county or environmental officials for laws and regulations in your area for proper disposal of these items. The county might provide a recycling center that will receive them. Before disposing of a monitor, first discharge the monitor.

Viruses and Other Computer Infestations

A+ OS 3.2

A computer support person needs to know how to protect computers against computer infestations (including viruses), how to recognize them, and how to get rid of them. Understanding what infestations are, how they work, and where they hide helps technicians deal with them successfully. A computer **infestation** is any unwanted program that is transmitted to a computer without the knowledge of the user or owner, and is designed to do varying degrees of damage to data and software. Computer infestations do not damage PC hardware, although, when boot sector information is destroyed on a hard drive, it can appear as though the hard drive is physically damaged. What most people refer to as viruses really fall into four categories of computer infestations: viruses, Trojan horses, worms, and logic bombs. The four types of infestations differ in the way they spread, what damage they do, and how they hide.

Because viruses are by far the most common of the four kinds of computer infestations, one of the most important defenses against computer infestations is **antivirus** (**AV**) software that is designed to discover and remove a virus. This section looks at several AV programs and how to use them effectively.

Understanding Computer Infestations

A+ OS 3.2

A **virus** is a program that can replicate by attaching itself to other programs. The infected program must be executed for a virus to run. The virus might then simply replicate, or also do damage by immediately performing some harmful action. A virus might be programmed to perform a negative action in the future, such as on a particular date (for instance, Friday the 13th), or when some logic within the host program is activated. A virus is different from a **worm**, a program that spreads copies of itself throughout a network without a host program. A **Trojan horse** is a third type of computer infestation that, like a worm, does not need a host program to work—rather it substitutes itself for a legitimate program. Trojan horses cannot replicate themselves. (This last statement has some exceptions. One Trojan horse program was disguised as an automatic backup utility downloadable from the Internet. When used, it created backups and replicated itself to the backups. It was programmed to damage several systems on Friday the 13th. In this case, the Trojan horse program is also considered a virus because of its ability to replicate.) A worm is seldom seen except on a network, where it creates problems by overloading the network as it replicates. Worms do damage by their presence rather than by performing a specific damaging act, as a virus does. A worm overloads memory or hard drive space by replicating repeatedly. Because Trojan horse infestations cannot replicate and require human intervention to move from one location to another, they are not as common as viruses.

Sometimes problems on a PC caused by an error or software bug can look and act like viruses, even when no virus is involved. Sometimes software is altered with malicious intent. A **logic bomb** is dormant code added to software and is triggered by a predetermined time or event. For example, an employee might put code into a program to destroy important files if his or her name is ever removed from the payroll file. Also, viruses, Trojan horses, logic bombs, and worms can occur in combination such as when a virus gains access to a network by way of a Trojan horse. The virus plants a logic bomb within applications software on the network that sets off a worm when it executes.

Where Viruses Hide

A program is called a virus because (1) it has an incubation period (does not do damage immediately), (2) it is contagious (can replicate itself), and (3) it is destructive. Viruses are often programmed to hide to avoid detection by antivirus software. A virus can hide in four ways. Sometimes a virus can use more than one method at the same time.

Boot Sector Virus A **boot sector virus** hides in a boot sector program. It can hide on a hard drive either in the program code of the Master Boot Record or in the boot record program that loads the OS on the active partition of the hard drive. On a floppy disk, a boot sector virus hides in the boot program of the boot sector. One of the most common ways a virus spreads is from a floppy disk used to boot a PC. When the boot program is loaded into memory, so is the virus, which can then spread to other programs.

However, a floppy disk does not have to be bootable to spread a virus. All floppy disks have a boot sector that contains a boot program. If a PC is configured to first boot from drive A then drive C, and a floppy disk is in the drive when the PC is booted, BIOS executes the boot program on the disk. If the disk is not bootable, this program displays an error message,

A+ OS 3.2

such as "Nonsystem disk or disk error." If the user removes the disk and presses any key, the PC boots from the hard drive. However, if the boot program of the floppy disk contains a boot sector virus, the virus might already have been loaded into memory. When the system boots from the hard drive, the virus is then spread to the boot sector of the hard drive.

To prevent this kind of infection, after unsuccessfully trying to boot from the floppy disk, don't press a key that instructs the PC to turn to the hard drive to boot. Also, pressing CTRL+ALT+DEL might not be enough to prevent the problem, because the loaded virus can still hide in memory and some viruses intercept a CTRL+ALT+DEL to take control of the PC. The best way to proceed is to use a cold boot—turn the PC off, remove the floppy disk, and turn the PC back on. The danger of virus infection from a floppy is a good reason to configure your computer to always boot from the hard drive first, and then, if the hard drive is not bootable, to boot from the floppy drive. This boot order normally prevents BIOS from reading a boot sector of a floppy disk that is inserted during boot. The order of booting from the A and C drives is determined in CMOS setup.

Incidentally, many CMOS setups have an option that prevents writing to the boot sector of the hard drive, which can protect against some boot sector viruses. This feature must be turned off before installing Windows 9x, Windows NT, or Windows 2000, which must write to the boot sector during installation. Windows 9x does not tell you that you must turn the feature off and start the installation over until about halfway through the installation.

File Viruses A **file virus** hides in an executable (.exe or .com) program or in a word-processing document that contains a macro. A **macro** is a small program contained in a document and can be automatically executed when the document is first loaded, or later by pressing a key combination. For example, a word-processing macro might automatically read the system date and copy it into a document when you open the document. Viruses that hide in macros of document files are called **macro viruses**. Macro viruses are the most common viruses spread by e-mail, hiding in macros of attached document files.

One well-known example of a macro virus is Melissa, first introduced on Friday, March 26, 1999, in a Word 97 macro. The virus immediately spread around the world within one working day. The e-mail that initially spread Melissa looked like this:

```
From: (name of infected user)
Subject: Important Message From (name of infected user)
To: (50 names from alias list)
Here is that document you asked for ... don't show anyone
else ;-)
Attachment: LIST.DOC
```

When the recipient opened the document, a macro executed and immediately e-mailed the LIST.DOC to 50 e-mail addresses listed in the user's address book. The virus infected other Word documents, which, when e-mailed, also spread the virus.

Melissa drops its payload, or activates, when a document is opened when the minutes of the hour match the day of the month (for example, at 09:18 on the 18th day of a month). It then inserts a phrase from the *Simpsons* TV show into the current document.

A+ OS 3.2

One type of file virus searches a hard drive for files with .exe file extensions and then creates another file with the same filename with a .com file extension, and stores itself there. When the user launches a program, the OS first looks for the program name with the .com file extension. It then finds and executes the virus. The virus is loaded into memory and loads the program with the .exe extension. The user appears to have launched the desired program. The virus is then free to do damage or spread itself to other programs.

A virus cannot work if it is contained in a data file with no embedded macros. Sometimes a virus copies itself to a data file by mistake, where it cannot do much damage, since the data is not a program and cannot be executed from memory. However, the virus can corrupt data by overwriting what was already in the file.

Multipartite Viruses A **multipartite virus** is a combination of a boot sector virus and a file virus. It can hide in either type of program.

Cloaking Techniques

A virus is programmed to attempt to hide from antivirus (AV) software. AV software can only detect viruses that are identical or similar to ones it has been programmed to search out and recognize. AV software detects a known virus by looking for distinguishing characteristics called the **virus signature**, which is why it is important to update your AV software.

TIP Antivirus software cannot detect a virus it does not know to look for. Therefore, continue to upgrade your AV software as new viruses are discovered.

A virus attempts to hide from AV software in two ways: by changing its distinguishing characteristics (its signature) and by attempting to mask its presence. Three types of viruses that are categorized according to their cloaking techniques are polymorphic, encrypting, and stealth viruses, which are discussed next.

Polymorphic Viruses A **polymorphic virus** changes its distinguishing characteristics as it replicates. Mutating in this way makes it more difficult for AV software to recognize the presence of the virus.

Encrypting Viruses One key symptom AV software looks for a program that can replicate itself. An **encrypting virus** can transform itself into a nonreplicating program to avoid detection. However, it must revert to a replicating program to spread or replicate, when it can be detected by AV software.

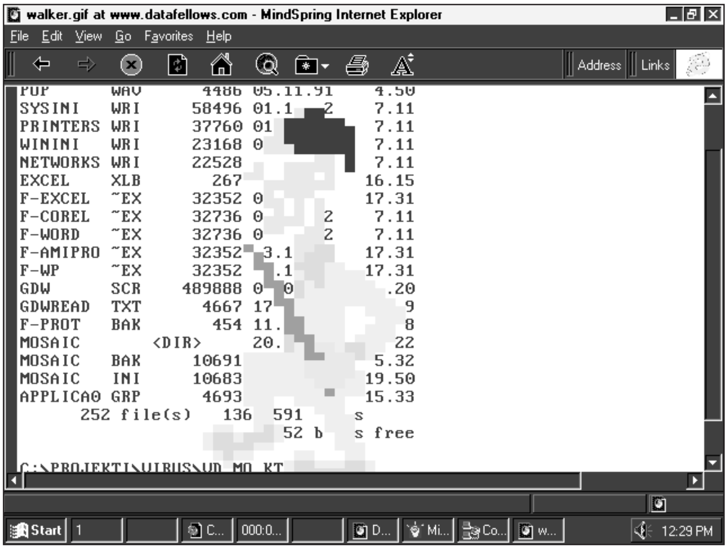
Stealth Viruses A **stealth virus** actively conceals itself, using one or more of the following techniques:

- Because AV software can detect a virus by noting the difference between a program's file size before the virus has infected it and after the virus is present, the virus alters OS information to mask the size of the file it is hiding in.

- The virus monitors when files are opened or closed. When it sees that the file it is hiding in is about to be opened, it temporarily removes itself or substitutes a copy of the file that does not include the virus. The virus keeps a copy of this uninfected file on the hard drive just for this purpose.

The Damage an Infestation Can Cause

Viruses, worms, and Trojan horses have not been known to physically damage a hard drive or other hardware device. The damage they do ranges from minor, such as displaying bugs crawling around on a screen, to major, such as erasing everything written on a hard drive. Infestation damage is called the payload and can be accomplished in a variety of ways. A virus can be programmed to drop its payload only in response to a triggering event such as a date, opening a certain file, or pressing a certain key. Figures 19-2 and 19-3 show the results of two harmless viruses that simply display garbage on the screen.


walker.gif at www.datafellows.com - MindSpring Internet Explorer
File Edit View Go Favorites Help
Address
Links
Start
1
C...
000:0...
D...
Mi...
Co...
w...
12:29 PM

```
PUP       WAV      4486 05.11.91     4.50
SYSINI    WRI     58496 01.1     2    7.11
PRINTERS  WRI     37760 01            7.11
WININI    WRI     23168 0             7.11
NETWORKS  WRI     22528               7.11
EXCEL     XLB       267              16.15
F-EXCEL   ~EX     32352 0            17.31
F-COREL   ~EX     32736 0        2    7.11
F-WORD    ~EX     32736 0        2    7.11
F-AMIPRO  ~EX     32352  3.1         17.31
F-WP      ~EX     32352   .1         17.31
GDW       SCR    489888 0  0           .20
GDWREAD   TXT      4667 17              9
F-PROT    BAK       454 11.             8
MOSAIC        <DIR>     20.            22
MOSAIC    BAK     10691               5.32
MOSAIC    INI     10683              19.50
APPLICA0  GRP      4693              15.33
      252 file(s)    136  591      s
                          52 b     s free

C:\PROJEKTI\VIRUS\VD MO KT
```

Figure 19-2 The harmless, or benign, Walker virus displays a man walking across the screen

How Infestations Spread

A+ OS 3.2

Understanding how infestations spread is essential to understanding how to protect your computer against them. Some computers are more vulnerable than others, depending on user habits. Below is a list of user activities that make a computer susceptible to infestations.

- Trading floppy disks containing program files
- Connecting the computer to an unprotected network
- Buying software from unreliable sources
- Downloading programs from the Internet

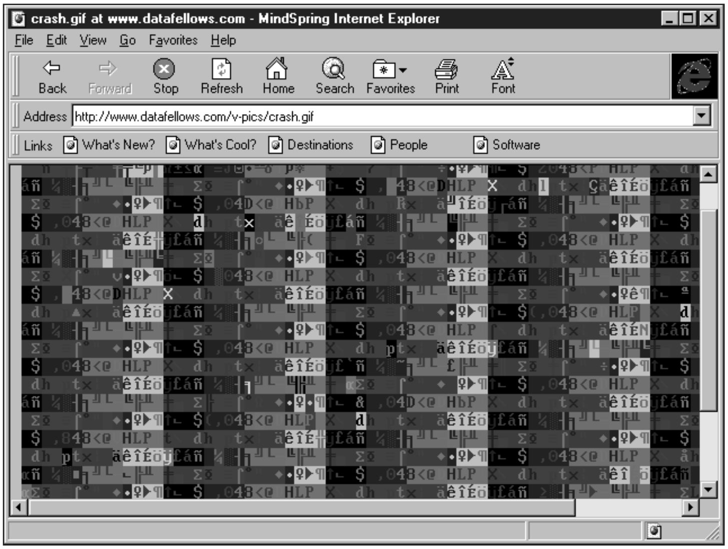

crash.gif at www.datafellows.com - MindSpring Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites Print Font
Address http://www.datafellows.com/v-pics/crash.gif
Links What's New? What's Cool? Destinations People Software

Figure 19-3 The crash virus appears to be destructive, making the screen show only garbage, but does no damage to the hard drive data

A+ OS 3.2

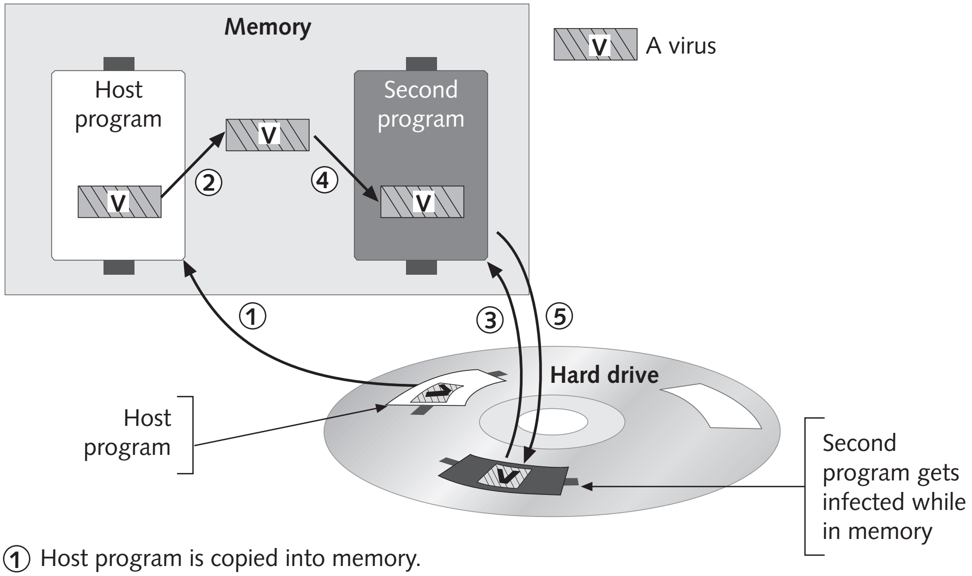
- Using floppy disks from unknown sources
- Using shared network programs
- Using used, preformatted floppy disks
- Reading e-mail that automatically executes a word processor to read attached files
- Not write-protecting original program disks

How a Virus Replicates Once a program containing a virus is copied to your PC, the virus can spread only when the infected program is executed. The process is shown in Figure 19-4. Recall from earlier chapters that the first step in executing a program, whether it is stored in a program file or in a boot sector, is to load the program into memory. Viruses hidden in a program can then be executed from memory. A virus can either be a **memory-resident virus** and stay in memory, still working, even after the host program is terminated, or a **non-memory-resident virus**, which means that it is terminated when the host program is closed.

After a virus is loaded into memory, it looks for other programs that are loaded into memory. When it finds one, it copies itself there and into that same program file on disk. From Figure 19-4, you can see that a virus becomes more dangerous the longer it stays loaded into memory and the more programs that are opened while it is there. For this reason, if you want to use a computer that has been used by other people, such as in a computer lab, always reboot before you begin work to clear memory of programs. Use a hard boot, not just a soft boot, to erase that all memory-resident programs (including a memory-resident virus) from memory.

A+ OS 3.2

TIP When using a computer in a computer lab, always hard boot the PC before you begin work to protect against viruses.



① Host program is copied into memory.

② The virus may or may not move itself to a new location in memory.

③ A second program is opened and copied into memory.

④ The virus copies itself to the second program in memory.

⑤ The newly infected second program is written back to the hard drive.

Figure 19-4 How a virus replicates

How a Trojan Horse Gets into Your Computer A Trojan horse is an infestation that masquerades as a legitimate program. One interesting example of a Trojan horse is the AOL4FREE program. Originally this was an illegal program that could provide unauthorized access to America Online. After the program's usefulness was blocked by AOL, a new program emerged, also called AOL4FREE, which was not an online access program, but a destructive Trojan horse. People passed the program around, thinking that it would provide illegal access to AOL; however, if executed, it actually erased files on their hard drives.

Virus Hoaxes A virus hoax is a letter or e-mail warning about a nonexistent virus. The warning is itself a pest because it overloads network traffic. Here's an example of a virus hoax e-mail message I received:

There is a new virus going around in the last couple of days!! DO NOT open or even look at any mail that you get that says: "Returned or Unable to Deliver." The virus will erase your whole hard drive and attach itself to your computer components and render them useless. Immediately delete any mail items that say this. AOL has indicated this is a very dangerous

A+ OS 3.2

virus, and there is NO remedy for it at this time. Please be careful and forward to all your online friends ASAP.This is a new email virus and not a lot of people know about it; just let everyone know, so they won't be a victim. Please forward this email to your friends!!!

First, don't believe the part about a virus rendering computer components useless. No virus has been known to actually do physical damage to hardware, although viruses can cause a PC to be useless by destroying programs or data. Second, don't believe the part that says the virus will be activated just because you open an e-mail message. An e-mail message is text, not a program, and a virus can't hide there. (It can, however, hide in word-processing documents containing macros that are attached to an e-mail message.) And third, don't be gullible and take the bait by forwarding the message to someone else. The potential damage a hoax like this can do is to overload an e-mail system with useless traffic, which is the real intent of the hoax. When I received this e-mail, there were over a hundred names on the distribution list.

Protecting Against Computer Infestations

You can do a lot to protect your computer against viruses and other infestations. Your first line of defense is to regularly make backups and use virus scan software. After that, use wisdom when managing programs. Here are some general guidelines:

- Buy antivirus software and set your computer to automatically run the AV program at startup.
- Keep your AV software current by periodically downloading upgrades from the Internet.
- Set a virus scan program to automatically scan word-processor documents as they are opened.
- Establish and faithfully execute a plan to make scheduled backups of your hard drive to protect against potential infestation damage.
- Only buy software from reputable vendors.
- Don't trade program files on floppy disks.
- Don't use floppy disks from unknown sources, and always scan floppy disks for viruses no matter where they came from.
- Download software from the Internet sparingly, and then *always* scan program files for viruses before executing them.
- Never use pirated software.
- Format floppy disks before first use.
- Write-protect original program disks.
- In a business environment, adopt strict company policies against using unauthorized software.

- Before using a running computer that others have already used, hard boot the computer.
- Set your computer CMOS settings to boot from drive C, then drive A.
- Turn on antivirus protection for your MBR in the CMOS settings, if available.

Virus Symptoms

A+ OS 3.2

Know what to expect when a virus is replicating or dropping its payload. Here are some warnings that suggest a virus is at work:

- A program takes longer than normal to load.
- The number and length of disk accesses seem excessive for simple tasks.
- Unusual error messages occur regularly.
- Less memory than usual is available.
- Files mysteriously disappear or appear.
- Strange graphics appear on your computer monitor, or the computer makes strange noises.
- There is a noticeable reduction in disk space.
- The system cannot recognize the hard drive when you have booted from a floppy disk.
- The system cannot recognize the CD-ROM drive, although it has worked earlier.
- Executable files have changed size.
- Executable files that once worked no longer work and give unexpected error messages.
- The access lights on the hard drive and floppy drive turn on when there should not be any activity on that device. (However, sometimes an OS will perform routine maintenance on the drive when the system has been inactive for a while.)
- Files constantly become corrupted.
- Strange or bizarre error messages appear.
- DOS or Windows error messages about the FAT or partition table are displayed.
- The hard drive boots but hangs up before getting a DOS prompt or Windows desktop.
- File extensions or file attributes change without reason.
- A message is displayed from the virus scanner software.
- The number of bad sectors on the hard drive continues to increase.
- The DOS MEM command reveals unfamiliar TSRs loaded into memory.

What to Do When You Suspect a Virus Infestation

If you suspect a virus, run a virus scan program to detect and delete the virus. If the antivirus software is not already installed, you can still use it. Consult the documentation for instructions on how to proceed. In many cases, the installation process detects the virus and eliminates it before continuing the installation. However, if the AV software does not recognize the virus, or if the virus successfully hides, the AV program cannot detect the virus. If the AV software found nothing, but you still suspect a virus, get the latest upgrade of your AV software and try it or another AV program.

Protecting Against Viruses

Antivirus software cannot prevent a Trojan horse program from being copied to your computer, tell you that an e-mail message is a hoax, or force you to use wisdom in handling software. However, aside from taking precautions to prevent a virus from entering your system, using antivirus software is your best line of defense against a virus. Table 19-3 lists some popular antivirus software and Web sites that provide information about viruses.

Table 19-3 Antivirus software and information

Antivirus Software and Information	Web Site
Command AntiVirus by Command Software Systems	*www.commandcom.com*
Datafellows (virus information)	*www.datafellows.com*
Dr. Solomon's Software	*www.drsolomon.com*
eSafe by Aladdin Knowledge Systems, Ltd.	*www.esafe.com*
F-PROT by FRISK Software International	*www.complex.is*
McAfee VirusScan by McAfee Associates, Inc. (a version is included on the CD-ROM with this book)	*www.mcafee.com*
NeaTSuite PC-cillin by Trend Micro	*www.antivirus.com*
Norton AntiVirus by Symantec Corporation	*www.symantec.com*
Patricia Hoffman's Virus Summary (virus information)	*www.vsum.com*

When selecting antivirus software, look for the ability to do the following:

- Download new software upgrades from the Internet so that your software knows about new viruses
- Automatically execute at startup
- Detect macros in a word-processing document as it is loaded by the word processor
- Automatically monitor files being downloaded from the Internet

19

Using Antivirus Software

A+ OS 3.2

Antivirus software can work at different times to scan your hard drive or a floppy disk for viruses. Most AV software can be configured to scan memory and the boot sector of your hard drive for viruses each time your PC is booted. Often it's not practical to have it scan

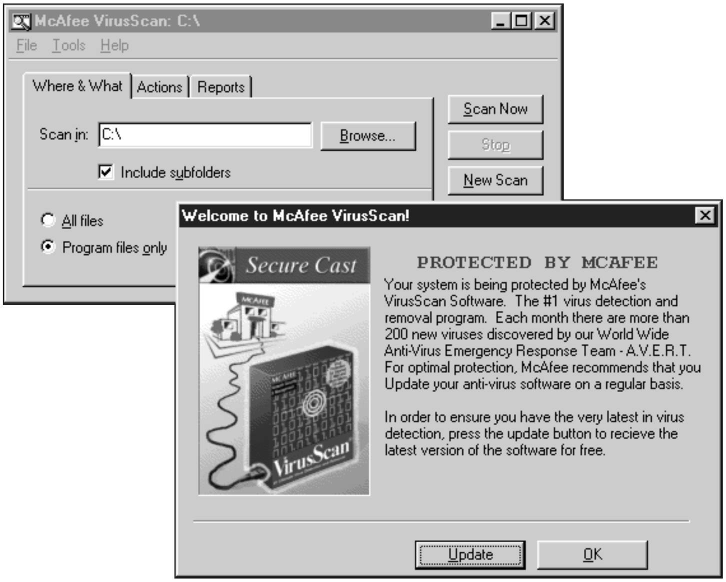
A+ OS 3.2

the entire hard drive each time you boot, because that takes too much time. Consider scheduling the AV software to run at the same time every day, such as during the lunch hour.

Some AV software can run continuously in the background and scan all programs that are executed. However, the software can cause problems with other software, especially during installations. If you are having a problem installing a new application, try terminating your AV software first.

Make sure your AV software can scan files as they are downloaded from the Internet or a network, and can scan documents for macro viruses each time a document is opened by a word processor. Make sure the AV software can scan both files and boot sectors of hard drives and disks. A version of McAfee VirusScan software is included with Nuts & Bolts on the CD-ROM accompanying this book. Using this software, follow these directions to scan a hard drive for viruses:

1. For Windows 9x, click **Start**, point to **Programs**, **Nuts & Bolts**, **McAfee VirusScan**, and then click **McAfee VirusScan**.
2. When the software first executes, it lets you log on to the McAfee web site and download any updates to the software (see Figure 19-5). You must be connected to the Internet before you click **Update** to download the files.



Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

PROTECTED BY MCAFEE

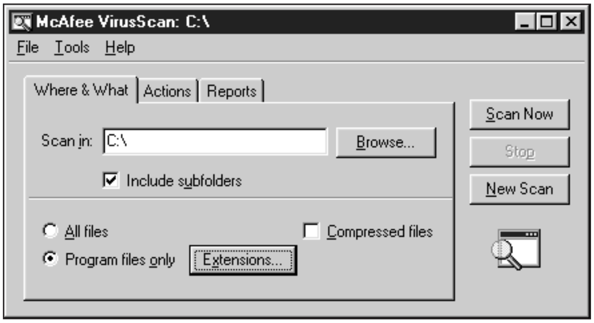
Your system is being protected by McAfee's VirusScan Software. The #1 virus detection and removal program. Each month there are more than 200 new viruses discovered by our World Wide Anti-Virus Emergency Response Team - A.V.E.R.T. For optimal protection, McAfee recommends that you Update your anti-virus software on a regular basis.

In order to ensure you have the very latest in virus detection, press the update button to recieve the latest version of the software for free.

Figure 19-5 McAfee VirusScan allows you to update the software from the McAfee Web site to ensure protection against newly discovered viruses

3. The McAfee VirusScan window opens, as shown in Figure 19-6. Select the drive to scan, what to do when a virus is detected, what reports to create and where, and what type of files to scan.

4. Click **Scan Now** to begin scanning.
5. Any viruses that are detected are listed in the box at the bottom of the screen.



Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

□ Compressed files

Figure 19-6 McAfee VirusScan software ready to perform a scan for viruses

All About Backups and Fault Tolerance

There's nothing like a rousing discussion of computer viruses to make a PC support person appreciate hard drive backups and other methods of protecting data. With data and software, a good rule of thumb is: if you can't get along without it, back it up. This section covers the hardware and software needed to make backups of data and software from a hard drive. Windows 9x, Windows NT, and Windows 2000 offer backup tools, which are also covered in this section. Another feature of preventive maintenance is to make hard drives more fault tolerant. **Fault tolerance** is the ability of a computer to respond to a fault or catastrophic event, such as a hardware failure or power outage, in such a way that data is not lost. Several approaches to making hard drives more fault tolerant are collectively called **RAID**. The term first stood for **redundant array of inexpensive disks**, but has recently been updated to mean **redundant array of independent disks**. The different methods of RAID are also discussed in this section.

Backup Hardware

Popular hardware devices used for making hard drive backups on standalone personal computers or small servers include tape, Zip, and Jaz drives, and read-write CDs. However, in a business environment, if a PC is connected to a file server, the most practical backup approach is to back up data from the PC's hard drive to the file server. Data on both the PC and the file server can become corrupted. However, the file server most likely uses its own automated backup utility to back up to either tape or a larger mainframe computer.

Regardless of the backup medium, it is practical to back up only the data and not the software on a regular basis. You might choose to back up software one time immediately after installation. Later, if the software becomes corrupted, it can be reinstalled.

This section first discusses using tape drives and then using removable drives for backups.

Tape Drives

Tape drives (Figure 19-7) are an inexpensive way of backing up an entire hard drive or portions of it. Tape drives are more convenient for backups than floppy disks or other types of removable disks, and they are relatively inexpensive. Tapes have capacities anywhere from several hundred kilobytes to several gigabytes and come in several types and formats. Although tape drives don't require that you use special backup software to manage them, most likely you will want to invest in specialized backup software to make backups as efficient and effortless as possible. Many tape drives come with bundled software. Several of the more common standards and types of tape drives and tapes are described in this section.

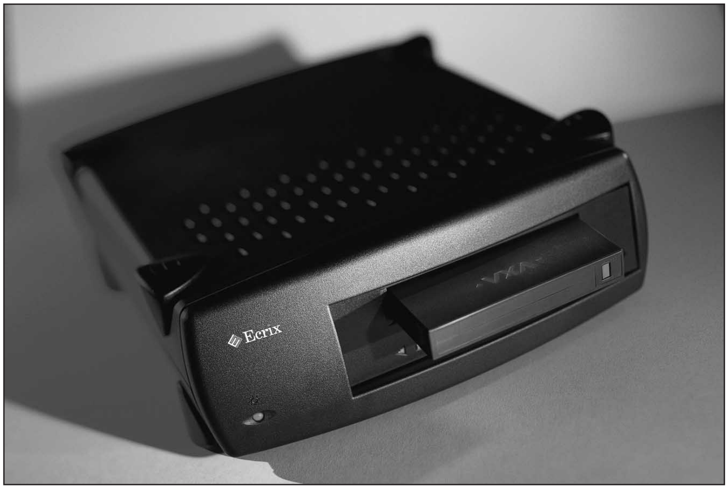


Figure 19-7 An external tape drive

The biggest disadvantage of using tape drives is that data is stored on tape by **sequential access**, meaning that, in order to read data from anywhere on the tape, you must start at the beginning of the tape and read until you come to the sought-after data. Sequential access makes recovering files slow and inconvenient, which is why tapes are not used for general-purpose data storage.

How a Tape Drive Interfaces with a Computer A tape drive can be external or internal. An external tape drive costs more but can be used by more than one computer. A tape drive can interface with a computer in these ways:

- An external tape drive can use the parallel port (see Figure 19-8) with an optional pass-through to the printer (so that the drive and the printer can use the same parallel port).

- An external or internal drive can use a SCSI bus. This method works well if the tape drive and the hard drive are on the same SCSI bus, which contains a data pass-through just to the SCSI system.
- An external or internal drive can use its own proprietary controller card or the floppy drive interface.
- An internal drive can use the IDE ATAPI interface.

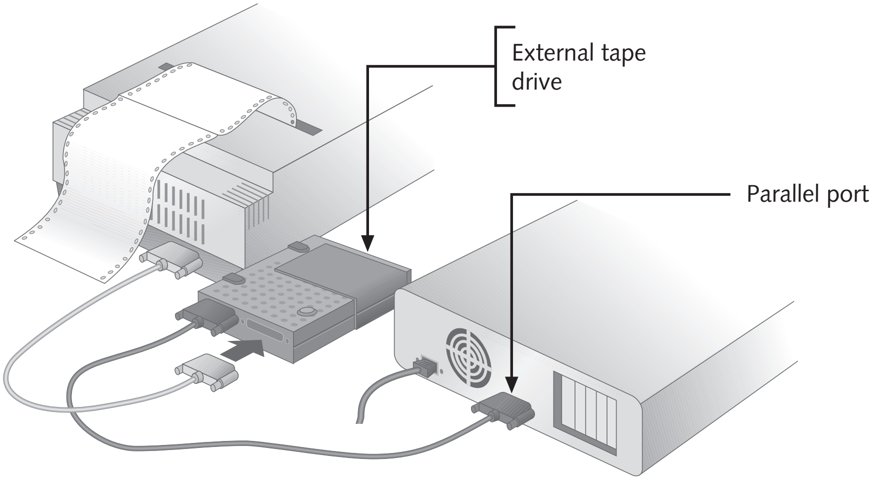


Figure 19-8 An external tape drive can use the parallel port for input/output, with an optional pass-through to the printer

Currently, the most popular tape drive interfaces are SCSI and IDE ATAPI. Figure 19-9 shows the rear of an ATAPI tape drive. You can see the connections for a power supply and 40-pin IDE cable and jumpers to set the drive to master, slave, or cable select. This setup is similar to any IDE device. When installing an ATAPI tape drive, avoid putting the drive on the same IDE data cable as the hard drive to prevent hindering the hard drive's performance. A typical configuration is to put the hard drive as the sole device on the primary IDE channel and put a CD-ROM drive and tape drive sharing the second channel. Set the CD-ROM drive to master and the tape drive to slave on that channel.

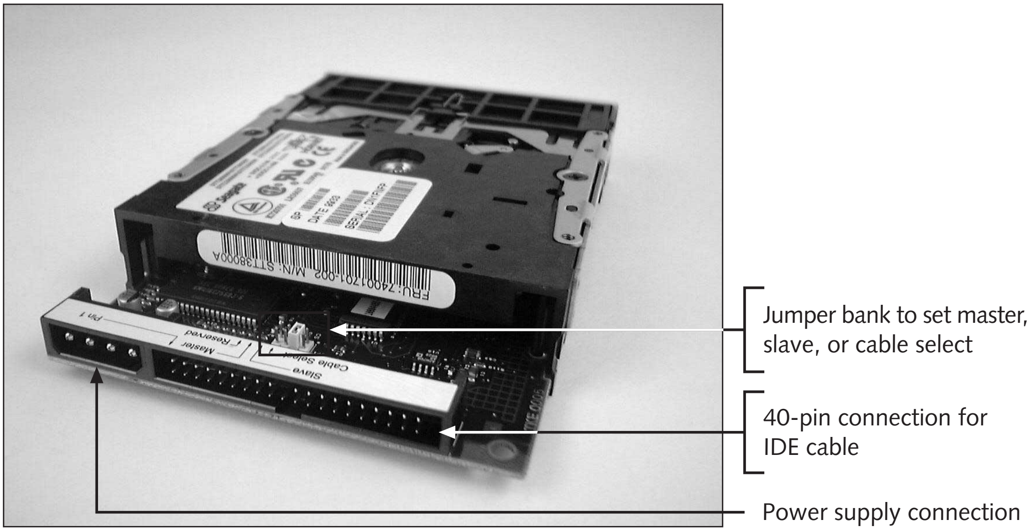

Jumper bank to set master, slave, or cable select
40-pin connection for IDE cable
Power supply connection

Figure 19-9 The rear of an ATAPI IDE tape drive

The Tapes Used by a Tape Drive Tape drives accommodate one of two kinds of tapes: full-sized **data cartridges** are 4 × 6 × ⅝ inches, and the smaller **minicartridges**, like the one in Figure 19-10, are 3¼ × 2½ × ⅗ inches. Minicartridges are more popular because their drives can fit into a standard 5½-inch drive bay of a PC case.

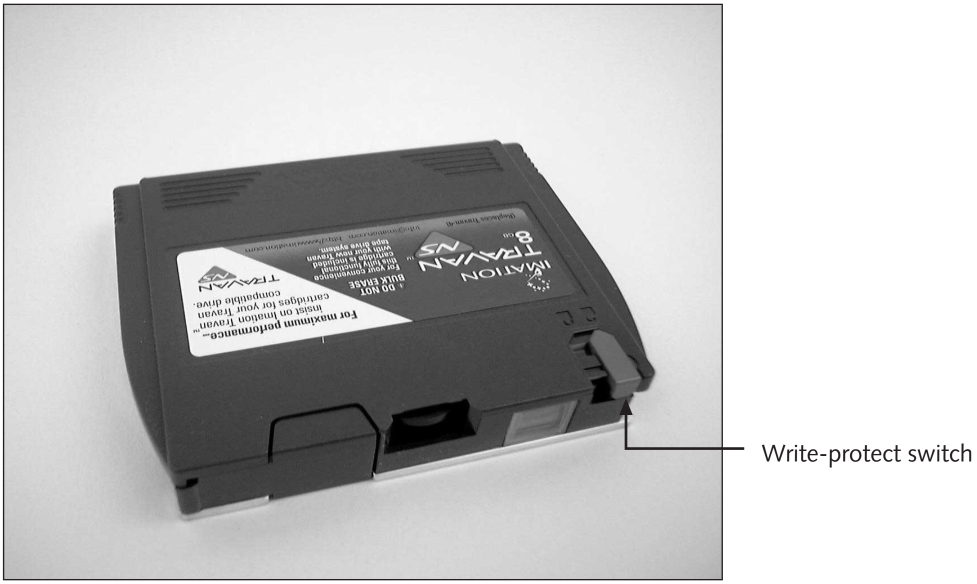


Figure 19-10 Minicartridge for a tape drive has a write-protect switch

The technology used by tape drives to write to tapes is similar to that used by floppy drives (see Chapter 5). A FAT at the beginning of the tape tracks the location of data and bad sectors on the tape. The tape must be formatted before data can be written to it. Buy factory formatted tapes to save time.

Standards for writing data to tapes have not developed as well as consumers would like, making it necessary to carefully match tapes to tape drives when purchasing and using them. Several standards exist, which have been promoted by different organizations as well as by individual manufacturers. Figure 19-11 shows two tables, each from a different tape drive manufacturer, showing the tape formats and tape types that are supported by their tape drives. Figure 19-11a shows that the Seagate Travan 8 or 20 GB drives that can support QIC-3080 and TR-5 tapes. Figure 19-11b shows that the Eagle TR-3 tape minicartridge tape drive can use either the QIC-3010 or QIC-3020 format and five tape types. Note that these drives are also likely to be able to read other formats that are compatible with these formats.

a) Tape formats for the Seagate Travan 8 GB and 20 GB tape drives

Tape Drive	Tape Format	Capacity	Tape Function
Travan NS 8 GB drive	Travan 8 (TR-4)	8 GB	Read and write
	QIC-3080	3.2 GB	Read and write
	QIC-Wide (3080)	4 GB	Read and write
Travan 20 GB drive	Travan 20 (TR-5)	20 GB	Read and write
	Travan 8 (TR-4)	8 GB	Read only

b) Minicartridge capacities obtained by the Eagle TR-3 tape drive using five different tape types

Tape Format	Travan TR-3	QIC Wide	MC 3000XL	TR-3 Extra	MC 3020 Extra
QIC-3020*	3.2 GB	1.7 GB	1.4 GB	4.4 GB	3.2 GB
QIC-3020	1.6 GB	850 MB	680 MB	2.2 GB	1.6 GB
QIC-3010*	1.6 GB	840 MB	680 MB	2.2 GB	1.6 GB
QIC-3010	800 MB	420 MB	340 MB	1.1 GB	800 MB

*Using software compression with an assumed 2:1 compression ratio

Figure 19-11 Tables from two tape drive manufacturers indicate the multitude of formats used when reading and writing to tapes

Tape Formats and Tape Types One of the first efforts to standardize the way data is written to tape was established around 1983 by a group of manufacturers who formed Quarter-Inch Cartridge Drive Standards, Inc. These standards are sometimes called the **Quarter-Inch Committee** (**QIC**), or quarter-inch cartridge (standards). Many QIC standards have been developed, but only a few are used today. 3M developed a standard, called Travan, based on the QIC format. Travan has been backed by many leaders in the tape drive industry. There are different levels of Travan standards, called TR-1 through TR-5, each based on a different QIC standard.

Looking at the second column of Figure 19-11a, showing tape types, and at the column headings of Figure 19-11b, you can see that there are several types of tape available. Although most manufacturers suggest that you use a tape cartridge they manufacture for their drive, tape drives often support a variety of tape types. Even though a tape drive can use a minicartridge rather than a data cartridge, not all minicartridge tapes can be used in any one drive. Consult the tape drive's user guide to find out which tape types you can use with the drive. Minicartridge tape drives use more than one type of tape drive mechanism, and more than one density is used to write data to a tape, just as there is more than one density for floppy disks. Also, some tape drives don't format tapes, meaning that you must buy preformatted tapes to use the drive.

Troubleshooting Guide for Tape Drives

A+CORE 2.2

The following is a list of possible tape drive problems you might encounter and suggestions for dealing with them.

A minicartridge does not work

- If you are trying to write data, verify that the minicartridge is write-enabled.
- Are you inserting the minicartridge correctly? Check the user guide.
- Check that you are using the correct type of minicartridge. See the user guide.
- Is the minicartridge formatted? The software performs the format and can take an hour or more.
- Retension the tape. Use the backup software to do this. Some tape drives require this, and others do not. **Retensioning** fast-forwards and rewinds the tape to eliminate loose spots.
- Take the minicartridge out and reboot. Try the minicartridge again.
- Try using a new minicartridge. The old one may have worn out.
- As with floppy disks, if the tape was removed from the drive while the drive light was on, the data being written at that time may not be readable.

Data transfer is slow

- Does the tape software have an option for optimizing speed or data compression? Try turning one, and then the other, off and on.
- Some tape drives can use an optional accelerator card to speed up data transfer. See the tape drive user guide.
- Try a new minicartridge.
- If the tape drive can do so, completely erase the tape and reformat it. Be sure that the tape drive can perform this procedure before you tell the software to do it.
- If you have installed an accelerator card, verify that the card is connected to the tape drive.
- Check that there is enough memory for the software to run.

A+ CORE 2.2

The drive does not work after the installation

- Check that pin 1 is oriented correctly to the data cable at both ends.
- Check for a resource conflict. The tape drive normally requires an IRQ, DMA channel, and I/O address.
- For DOS, check the entries in CONFIG.SYS and AUTOEXEC.BAT.

The drive fails intermittently or gives errors

- The tape might be worn out. Try a new tape.
- Clean the read/write head of the tape drive. See the tape drive user guide for directions.
- For an external tape drive, move the drive as far as you can from the monitor and computer case.
- Reformat the tape.
- Retension the tape.
- Verify that you are using the correct tape type and tape format.

Removable Drives

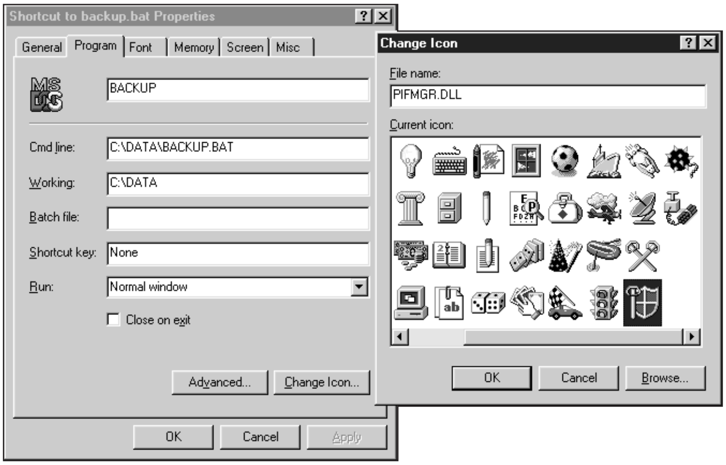
A+ OS 1.3

New media such as read-writable CDs or Jaz drives are becoming popular for PC backups because they can be used for other purposes as well, and because their prices have recently been reduced. As discussed in Chapter 6, Zip drives come in 100-MB or 250-MB sizes. SuperDisk holds 120 MB of data, and Jaz drives hold 1 GB or 2 GB of data. These removable drives are ideal for backups as long as the data fits on one disk. When data can fit on a single removable disk, a quick and easy method of backing up data to one of these disks is to create a shortcut on your desktop that executes a small batch file (text file with .BAT file extension). The example below demonstrates how to create a shortcut to back up the \Data directory, its files, and subdirectories:

1. Using Notepad or WordPad, type this command line, where the removable drive is E and the /S parameter tells the OS to include subdirectories when copying (Hidden files will not be copied, but data is not usually hidden.):

   ```
   XCOPY C:\DATA\*.* E: /S
   ```

2. Save the file as **\Data\BATCH.BAT** and exit the editor.
3. Create a shortcut to the BATCH.BAT file.
4. Since .BAT files are DOS files, the icon on the desktop will be the MSDOS icon. To change the icon, right-click the icon, select **Properties** from the shortcut menu, click the **Program** tab, and click **Change Icon** (see Figure 19-12). Select an icon, then click **OK** twice to return to the desktop.



BACKUP

Cmd line: C:\DATA\BACKUP.BAT

Working: C:\DATA

Batch file:

Shortcut key: None

Run: Normal window

□ Close on exit

File name: PIFMGR.DLL

Current icon:

Figure 19-12 Change the icon for the BACKUP.BAT shortcut

5. Whenever you want to back up your data, place a disk in the drive and double-click the shortcut icon.

TIP

The batch file just created is very simple and only uses DOS commands. Window
a much more sophisticated tool, Windows Scripting Host (WSH), to execute scri
programmers have written using a scripting language such as VBScript or JScri
script is stored in a file that can be placed as an icon on the desktop. To run
script, type **wscript.exe filename** in the Run dialog box, substituting filename w
name of the script file or double-click on the desktop icon.

Backup Methods

You can use more sophisticated methods to create backups in which the backup process is selective, only backing up what's changed, what has not been recently backed up, and so forth. Traditionally, these methods all involve backing up to tapes, because a tape is more likely to be large enough to contain an entire backup. In discussing these methods, we use tapes as our medium. These backup methods are designed to reuse tapes and to make the backup process more efficient. The child, parent, grandparent method is a plan for reusing tapes. Full, incremental, and differential backup methods speed up the backup process, and scheduled backups minimize the inconvenience to users. Selective backups only back up data that changes often on the hard drive. By selecting only certain critical folders on the drive to back up, the backup routine goes much faster, and recovery of lost data is much easier.

The Child, Parent, Grandparent Method

Before you perform routine hard drive backups, devise a backup plan or procedure. One common plan, called the **child, parent, grandparent method**, makes it easy to reuse tapes. This method is explained in Table 19-4. Put the plan in writing and keep a log of backups performed.

Table 19-4 The child, parent, grandparent backup method

Name of Backup	How Often Performed	Storage Location	Description
Child backup	Daily	On-site	Keep four daily backup tapes and rotate them each week. Label the four tapes Monday, Tuesday, Wednesday, and Thursday. A Friday daily (child) backup is not made, because on Friday you'll make the parent backup.
Parent backup	Weekly	Off-site	Perform the weekly backup on Friday. Keep five weekly backup tapes, one for each Friday of the month, and rotate them each month. Label the tapes Friday 1, Friday 2, Friday 3, Friday 4, and Friday 5.
Grandparent backup	Monthly	Off-site, in a fireproof vault	Perform the monthly backup on the last Friday of the month. Keep 12 tapes, one for each month. Rotate them each year. Label the tapes January, February, and so on.

Full, Incremental, and Differential Backups

A+ OS 1.3

Some backup methods are more efficient because they do not always create a complete backup of all data. A **full backup** backs up all data from the hard drive. An **incremental backup** backs up only files that have changed or that have been created since the last backup, *whether that backup is itself an incremental or full backup*. **Differential backups** back up files that have changed or been created since the last *full* backup.

Begin by performing a full backup. The next time you back up, choose the incremental method to back up only files that have changed or been created since the full backup. The second time you perform an incremental backup, you back up only the files that have changed or been created since the last incremental backup.

For example, using the child, parent, grandparent method, you can perform a full backup each Friday. Monday through Thursday, you perform incremental backups. The advantage of this method is that incremental backups are faster and require less tape space than full backups. The disadvantage is that, to recover data, you must begin with the last full backup and work your way forward through each incremental backup until the time that the data was lost. This process can be time consuming. Plan to make a full backup after at least every sixth or seventh incremental backup. The Windows 9x, Windows NT, and Windows 2000 backup utilities support incremental backups.

If you create differential backups with the child, parent, grandparent method, create a full backup on Fridays. On Monday, do a differential backup to back up all files that have changed since Friday. On Tuesday, a differential backup also backs up all files that have changed since Friday (the full backup). Differential backups don't consider whether other differential backups have been performed, but compare data only to the last full backup, which is how differential backups and incremental backups differ. Another difference is that incremental backups mark files as backed up by clearing the archive bit in the attribute byte, but the differential backup does not mark a file as having been backed up. The advantage of differential backups over incremental ones is that if you need to recover data, you only need to recover from the last full backup and the last differential backup. Differential backups are not supported by Windows 95, but are supported by Windows 98, Windows NT, and Windows 2000.

Scheduling Backups

A+ OS 1.3

Backups can be performed manually by a user sitting at the computer or can be scheduled to run automatically without user interaction. A scheduled backup is automatically performed by software when the computer is commonly not in use, such as during the middle of the night. Windows 98, Windows NT, and Windows 2000 support scheduling any program (including backup tasks) to execute at designated dates and times without user intervention. Using Windows 98, do the following to schedule the BATCH.BAT program created earlier in the chapter to run at 11:59 p.m. every Monday night:

1. Double-click **My Computer** on the desktop, and then double-click **Scheduled Tasks** to open the Scheduled Tasks window (see Figure 19-13).

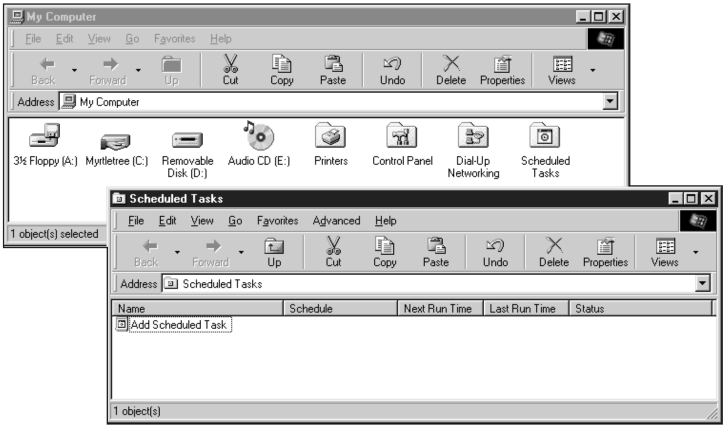


Figure 19-13 Add a scheduled task under Windows 98

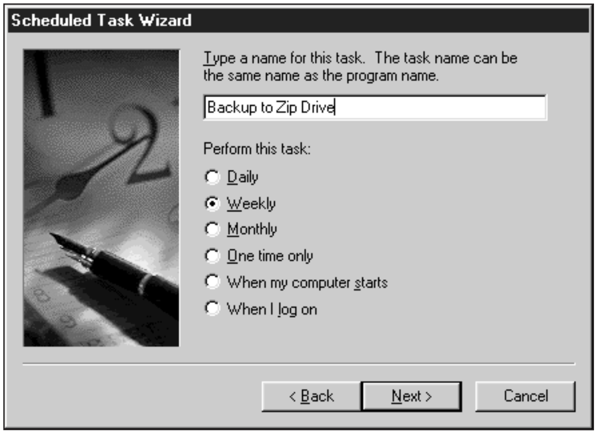
2. Double-click **Add Scheduled Task**. The Scheduled Task Wizard appears (see Figure 19-14). Select the program to schedule: Click **Browse**, find and click the **BATCH.BAT** file in the \Data folder, and click **Open**.

3. Enter a name for the scheduled task, select how often to perform the task, and then click **Next**.

4. Enter the start time and select the day of the week for the task to execute. For example, enter **11:59 PM every Monday**. Click **Next**.

5. The wizard reports the scheduled task parameters. Click **Finish**.

A+ OS 1.3



Type a name for this task. The task name can be the same name as the program name.

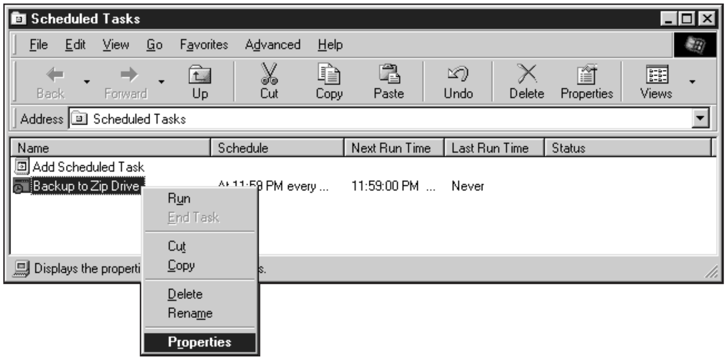
Backup to Zip Drive

Perform this task:

○ Daily
● Weekly
○ Monthly
○ One time only
○ When my computer starts
○ When I log on

Figure 19-14 Name the scheduled task and select how often it runs

6. To change the settings for a scheduled task, double-click **My Computer**, double-click **Scheduled Tasks**, and right-click the task in the Scheduled Task window. Select **Properties** from the shortcut menu (see Figure 19-15). The task Properties dialog box opens (see Figure 19-16).



Address Scheduled Tasks

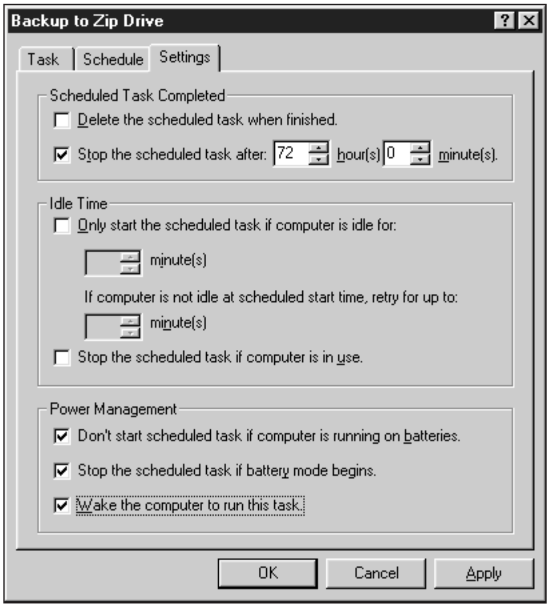
Name	Schedule	Next Run Time	Last Run Time	Status
Add Scheduled Task				
Backup to Zip Drive	At 11:59 PM every ...	11:59:00 PM ...	Never	

Displays the properti... s.

Figure 19-15 To change the task settings, use the Properties box of the task listed in the Scheduled Tasks window

7. Click the **Settings** tab to change the task settings. Notice at the bottom of the Settings sheet that you can direct the scheduler to wake the computer to perform the task. This feature requires a system board that supports the option for software to power up the PC. To know if your system board supports the feature, see CMOS setup or the system-board documentation. If not, then the PC must be turned on for the scheduler to work.

A+ OS 1.3



Backup to Zip Drive

Scheduled Task Completed

☐ Delete the scheduled task when finished.

☑ Stop the scheduled task after: 72 hour(s) 0 minute(s).

Idle Time

☐ Only start the scheduled task if computer is idle for:

minute(s)

If computer is not idle at scheduled start time, retry for up to:

minute(s)

☐ Stop the scheduled task if computer is in use.

Power Management

☑ Don't start scheduled task if computer is running on batteries.

☑ Stop the scheduled task if battery mode begins.

☑ Wake the computer to run this task.

Figure 19-16 With some computers, the task scheduler can power up the computer to run the task

Backup Software

A+ OS 1.3

Most tape drives come with some backup software.You can also purchase third-party backup software or use Windows 9x, Windows NT, or Windows 2000 for backing up your hard drive. Because the software only backs up files that are not currently in use, close all files before performing a backup.

Windows 9x Backup Utility

Windows 9x offers a backup utility that can back up to floppy disks and tape drives. Windows 98 supports many popular backup devices that Windows 95 did not, including those using parallel ports, IDE/ATAPI, and SCSI devices. To use drives and tapes not supported by Windows 9x, you also must use third-party backup software.

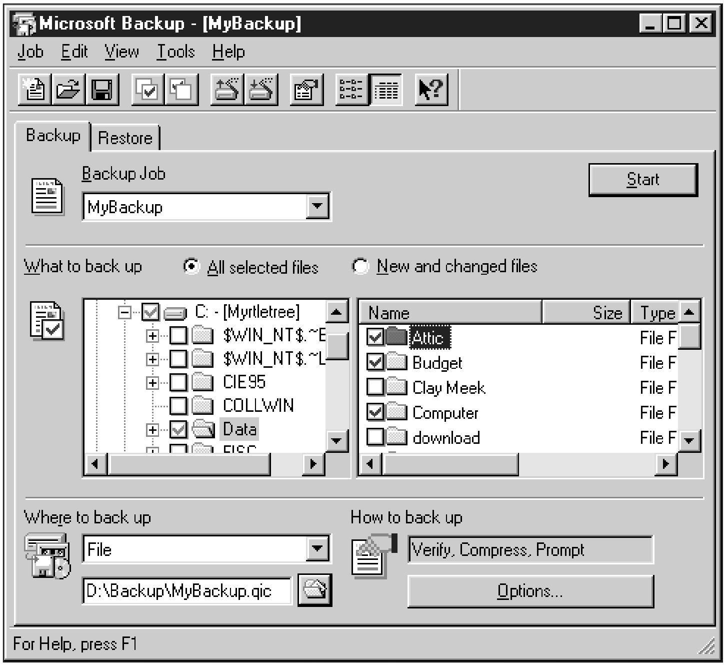
If the Windows 9x Backup component is not installed under Windows 9x, you can install it as follows:

1. Click **Start**, point to **Settings**, click **Control Panel**, and double-click **Add/Remove Programs**.
2. Click the **Windows Setup** tab.
3. Under **Disk Tools** for Windows 95 or **System Tools** for Windows 98, select **Backup**. Click **OK** and then click **Apply** to install the component. Supply the original Windows 9x floppy disks or CD so that the OS can complete the installation.

A+ OS 1.3

To use the Windows 98 Microsoft Backup utility, do the following:

1. Click **Start**, point to **Programs**, **Accessories**, **System Tools**, and click **Backup**. The Backup Wizard first searches for backup devices such as Zip or tape drives. If it finds none, it asks if you want to install one. Otherwise, it displays a window asking if you want to create a new backup job or open an existing job. The Backup utility keeps information about backup jobs under a name that you give it, so you can use the same job many times. Select **Create a new backup job** and click **Next** to continue.
2. The Backup Wizard asks you questions about what type of backup you want (for example, back up all files or only those files that have changed since the last backup). Make your selections and then click **Next**.
3. The Microsoft Backup utility opens the Backup window, as shown in Figure 19-17.



Backup Job: MyBackup

What to back up: ● All selected files ○ New and changed files

☑ C: - [Myrtletree]
□ WIN_NT.~B
□ WIN_NT.~L
□ CIE95
□ COLLWIN
☑ Data
□ FISC

Name	Size	Type
☑ Attic		File F
☑ Budget		File F
□ Clay Meek		File F
☑ Computer		File F
□ download		File F

Where to back up: File
D:\Backup\MyBackup.qic

How to back up: Verify, Compress, Prompt

For Help, press F1

Figure 19-17 Windows 98 Microsoft Backup allows you to select files and folders to back up

4. To back up only certain folders, files, or logical drives, check the boxes to the left of their names. To display a list of all subfolders under a folder, click the box with the + sign in it. Backup indicates that only parts of a folder or drive are selected for backup by placing a gray check in the box.

A+ OS 1.3

5. From the **Where to back up** list box of the Backup window shown in Figure 19-17, select the medium and directory to use. In the figure the medium is drive D, a Zip drive. The backup file will go into a folder named \Backup.
6. Click **Start** to begin the backup.

To recover files, folders, or the entire hard drive from backup using the Windows 98 Backup utility, follow these directions:

1. On the Backup utility window, shown in Figure 19-17, click the **Restore** tab. Select the backup job to use for the restore process. The Backup utility displays the folders and files that were backed up with this job. You can select the ones that you want to restore.
2. Click **Start** to restore the files.

Disk Cloning Software

You can back up a hard drive to replicate the drive to a new computer, such as when you deploy a new operating system with applications software on multiple computers in a corporate or educational lab. This process is called **disk cloning** or **disk imaging** and is best done with software designed for that purpose. Examples of disk imaging software are Drive Image by PowerQuest (see *www.powerquest.com)*, ImageCast by Innovative Software (see *www.imagecast.com)*, and Norton Ghost by Symantec Corp (see *www.symantec.com*).

RAID

Besides maintaining good backups, you can also protect data by continuously writing two copies of the data, each to a different hard drive. This method is most often used on high-end, high-cost file servers, but it is occasionally appropriate for a single-user workstation.

Collectively, these several methods, used to improve performance and/or automatically recover from a failure, are called RAID (redundant array of independent disks). There are several levels of RAID, but this section discusses only the three most commonly used (Table 19-5). Only the first level is financially practical for a standalone workstation.

RAID Level 0 increases the logical drive capacity by treating two drives as a single logical drive, but it includes only one copy of data. Therefore, it does not let you recover from a failure (an important feature of fault tolerance). RAID 0 is one method of **disk striping**, in which more than one hard drive is treated as a single volume. For an array of two hard drives, some data is written to one hard drive and some to the other; both drives make up one logical drive, or volume, and data is only written once. RAID 0 is supported by Windows NT and Windows 2000, but not by Windows 9x.

RAID Level 1 is designed to protect data from a hard drive failure by writing the data twice, once to each of two drives. One type of RAID Level 1 is called **disk mirroring**, in which the two hard drives both use the same adapter card.

Table 19-5 The three most common RAID levels

RAID Level and Common Name	Intended Purpose	Description
RAID 0: Disk striping without parity (striping refers to writing data across more than one physical drive)	Increases system performance and volume capacity	Data is written to two or more hard drives. The set of drives is treated as a single volume (a single virtual drive). Because more than one drive is doing the work, performance improves.
RAID 1: Disk mirroring or disk duplexing	Provides fault tolerance	Data is written twice, once to each of two drives. Disk mirroring uses only a single HD adapter. Disk duplexing uses two adapters, one for each drive.
RAID 5: Disk striping with parity	Increases performance and volume capacity and provides fault tolerance	Data is written to three or more drives, and parity information is distributed across these drives so that, if one drive fails, the other drives can re-create the data stored on the failed drive.

The advantages of RAID 1 disk mirroring are:

- If either drive fails, the data is still safe on the other drive.
- Disk reads are speeded up because the adapter has two places to read from.

The disadvantages of RAID 1 are:

- Having two hard drives in the same computer is more expensive.
- Because the data is written twice, hard drive capacity is, in effect, cut in half.
- Disk writes are slowed down because the data must be written twice.

One weakness in drive mirroring is that both hard drives are using the same adapter. If the adapter fails, neither hard drive is accessible. An improvement of disk mirroring, also considered RAID 1, is **duplexing**, in which each hard drive has its own adapter card. The initial cost is higher, but if one adapter fails, you are protected from losing the data on both drives. If a workstation cannot backup to a server on a network, disk mirroring or duplexing might be appropriate (if the data is considered valuable enough to merit the added expense).

Windows NT Workstation does not support RAID 1, so to use it on a workstation, the two hard drives must be managed by firmware on the controllers rather than by the OS. The more sophisticated hard drive controller increases the hardware expense. Windows NT Server supports RAID 1 and RAID 5.

RAID 5, or disk striping with parity, is an interesting variation of RAID 0 combined with RAID 1 and RAID 4, and improves fault tolerance and drive capacity. RAID 5 requires at least three hard drives. To understand RAID 5, we must first examine how RAID 4 works. In Figure 19-18, RAID 4 uses four hard drives grouped as one virtual hard drive. When any data is written to this one drive, the data is divided into three segments. Each segment is written to one of the first three drives, and parity information about the three segments is written to the fourth drive.

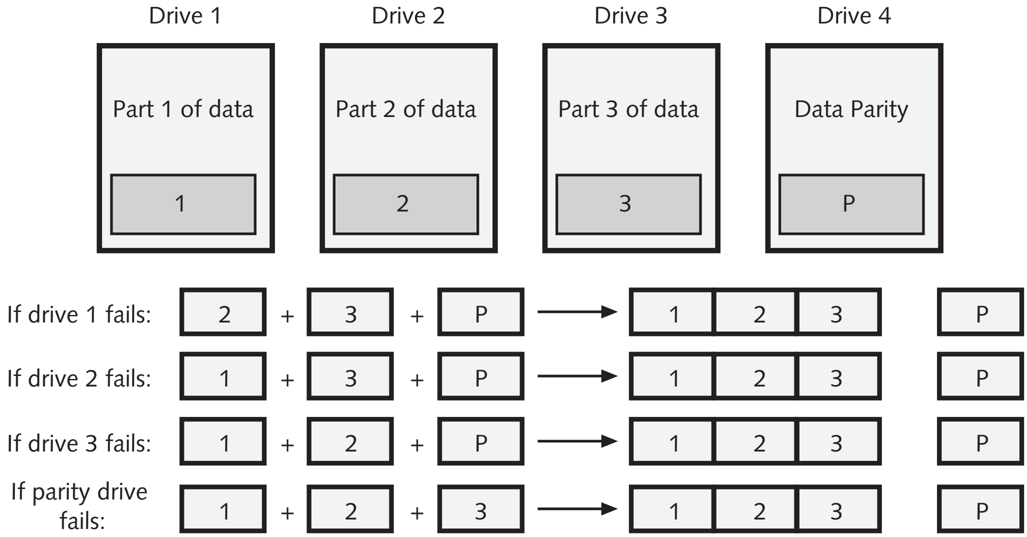

Drive 1
Drive 2
Drive 3
Drive 4
Part 1 of data
1
Part 2 of data
2
Part 3 of data
3
Data Parity
P
If drive 1 fails: 2 + 3 + P → 1 2 3 P
If drive 2 fails: 1 + 3 + P → 1 2 3 P
If drive 3 fails: 1 + 2 + P → 1 2 3 P
If parity drive fails: 1 + 2 + 3 → 1 2 3 P

Figure 19-18 RAID 4, disk striping with parity, allows for increased drive capacity as well as fault tolerance: any one drive can fail and data can still be re-created

If any of the four drives fails, the data can be recovered from the other three drives using the method illustrated in the lower half of Figure 19-18. Using any two segments and the parity information, the three segments can be recreated, or, if the parity drive fails, the three segments are still safely stored on the first three drives. With RAID 5, rather than storing all parity information on a single, dedicated parity drive, parity information is distributed over all the drives, thus removing the performance bottleneck created by having a single parity drive.

To understand how data is recovered using parity information, consider this simple example. Suppose three numbers are stored on three different drives. If you store the sum of the three numbers on the fourth, or parity, drive, you can use the information you have to calculate a missing number. For example, let's say the three numbers are 1, 2, and 6, you store their sum (9) on the parity drive. If the first number is lost, you can calculate it from the sum and the other two numbers.

When a drive fails, the data can be regenerated on the replacement drive using information from the other drives. First replace the failed drive with a new drive. To generate the data on the new drive when using Windows NT Server, go to the Disk Administrator of the Administrator Tools and execute a Regenerate command. Windows NT does the rest. The action is automatic, and you can still use the computer for other operations while regenerating is taking place.

For file servers using RAID 5 that must work continuously, it might be practical to use hardware that allows for hard drive hot swapping, which means that you can remove one hard drive and insert another without powering down the computer. However, hard drives that can be hot swapped cost significantly more than regular hard drives.

Windows 2000 Dynamic Drives

Windows 2000 offers a new feature called dynamic drives that protects the information stored in partition tables of traditional drives. (Using Windows 2000 terminology, hard drives that use partition tables are called **basic drives**.) Recall from earlier chapters that the partition table shares the same first sector at the beginning of the drive with the master boot program. Because the master boot program is often the target of boot sector viruses, the partition table is vulnerable to attack. Windows 2000 solves this by storing information about partitions in a 1-MB database written at the end of the hard drive, rather than at the beginning. The hard drive is then called a **dynamic drive** and the partitions are called **volumes**. When you upgrade a hard drive from basic to dynamic, the information in the partition table is moved to the database at the end of the drive. DOS and Windows 9x can have only two partitions; Windows NT can have up to four, but Windows 2000 can have up to 26 volumes, limited only by the number of letters in the alphabet.

Windows 2000 Professional can also link several volumes spread across multiple hard drives, called **spanned volumes**, which creates one logical drive. Windows 2000 Professional supports RAID 0 and calls it a striped volume. In addition to spanned volumes and striped volumes, Windows 2000 Server supports RAID 1, which it calls a mirrored volume, and RAID 5, which it calls RAID-5 volume.

To create any type of RAID volume under Windows 2000, you must use dynamic drives, although, if you are upgrading from Windows NT to Windows 2000 and already have a RAID system set up, Windows 2000 supports the setup using basic drives. The primary advantage of using dynamic drives over basic drives is that the 1-MB database not only contains information about the volumes on its hard drive, but also automatically contains information about all volumes on all hard drives in the system. This database is automatically replicated on all drives. If one database fails, it is quickly and automatically restored using a copy of the database on another drive. Dynamic drives have little advantage for a system with only a single hard drive, especially considering that only Windows 2000 can read dynamic drives.

Planning for Disaster Recovery

The time to prepare for a disaster is before it occurs. If you have not prepared, the damage from a disaster will probably be greater than if you had made and followed disaster plans. Suppose the hard drive on your PC stopped working and you lost all its data. What would be the impact? Are you prepared for this event? Backups are important, but you should also know how to use them to recover lost data. Also know when the backup was made and what to do to recover information entered since the last backup. Here's where careful record-keeping can pay off.

When you perform a backup for the first time or set up a scheduled backup, verify that you can use the backup tape or disks to successfully recover the data. This is a very important step in preparing to recover lost data. After you have created a backup tape, erase a file on the hard drive, and use the recovery procedures to verify that you can recreate the file from the backup. This verifies that the tape or floppy disk works, the recovery software is effective, and that you know how to use it. After you are convinced that the recovery works, document how to perform the recovery.

TIP Verify that your recovery plan will work by practicing it before a disaster occurs.

Always record your regular backups in a table with the following information: the folders or drives backed up, the date of the backup, the type of backup, and the name of the tape used. Refer to this table to recover data that was lost days or weeks before you discovered that should be recovered. Keep the records in a notebook. You can also store the records in a log file (a file where events are logged or recorded) each time you back up; always keep hard copies of log files in a paper file. The log-file method might be too time-consuming to do daily. Even though the software automatically records events to the log file, the backup will take longer because of the extra writing, and printing the file later will also consume time.

Periodically fully restore a hard drive that you back up. Use the tape made from a full backup and a different hard drive. Restore the first hard drive to the new hard drive and compare the results so you are confident that your backups can recover from a disaster.

CHAPTER SUMMARY

- PC failures are caused by many environmental and human factors, including heat, dust, magnetism, power supply problems, static electricity, spilled liquids, viruses, and human error.
- The goals of preventive maintenance are to make PCs last longer and work better, protect data and software, and reduce the cost of repairs.
- A PC preventive maintenance plan includes blowing dust from the inside of the computer case, cleaning the contacts on expansion cards, keeping a record of setup, backing up the hard drive, and cleaning the mouse, monitor, and keyboard.
- Protecting software and hardware documentation is an important preventive maintenance chore.
- Never ship a PC when the only copy of important data is on its hard drive.
- Computer infestations include viruses, Trojan horses, and worms, which are categorized by how they are transmitted.
- Antivirus software is your best defense against the damage caused by viruses.
- Viruses can hide in program files, boot sectors, and documents that contain macros. They attempt to cloak themselves from antivirus software by changing their distinguishing characteristics and masking their presence.

- Some viruses are relatively harmless, only displaying garbage on the computer screen. Others can be so destructive they erase everything on a hard drive, including partition table information.
- Steps you can take to prevent viruses from infesting your computer include not trading floppy disks, buying software from reliable sources, downloading programs from reliable sites on the Internet, and using networks with caution.
- A virus hoax is intended to overload network traffic. It works by tricking people into forwarding e-mail messages about viruses.
- To protect against damage by viruses, use antivirus software and back up your hard drive regularly.
- Tape drives are the most common hardware devices used to back up a hard drive, and come in many types and formats.
- Use RAID (redundant array of independent disks) to mirror data stored on a hard disk and to increase hard drive capacity by making more than one hard drive work as a single virtual drive.
- Use the child, parent, grandparent method of backing up data to reuse tapes according to a straightforward and easy-to-follow plan.
- Using a full backup, followed by incremental or differential backups, speeds up the time it takes to make a backup.
- Scheduled backups are performed when no one is using the computer.
- Windows 9x, Windows NT and Windows 2000 include a Backup utility that can be used with tape drives. In addition, Windows 9x Backup can use floppy disks, and Windows 2000 Backup can use several types of storage media including those on a network.
- When planning for disaster recovery, keep careful records of backups and periodically test your backup method to ensure that you can successfully recover lost data. Have a written disaster recovery plan.

KEY TERMS

Antivirus (AV) software — Utility programs that prevent infection, or scan a system to detect and remove viruses. McAfee Associates VirusScan and Norton AntiVirus are two popular AV packages.

Basic drive — In Windows 2000, a drive that uses a partition table at the beginning of the drive to hold information about the drive's primary and extended partitions. Compare to dynamic drive.

Boot sector virus — An infectious program that can replace the boot program with a modified, infected version of the boot command utilities, often causing boot and data retrieval problems.

Child, parent, grandparent backup method — A plan for backing up and reusing tapes or removable disks by rotating them each week (child), month (parent), and year (grandparent).

Data cartridge — A type of tape medium typically used for backups. Full-sized data cartridges are 4 × 6 × ⅝ inches in size. A minicartridge is only 3¼ × 2½ × ⅗ inches.

Differential backup — Backs up only files that have changed or have been created since the last *full* backup. When recovering data, only two backups are needed: the full backup and the last differential backup.

Disk cloning — Making an exact image of a hard drive including partition information, boot sectors, operating system installation and applications software to replicate the hard drive on another system or recover from a hard drive crash. Also called disk imaging.

Disk duplexing — An improvement of disk mirroring, whereby redundant data is written to two or more drives, and each hard drive has its own adapter card. This provides greater protection than disk mirroring.

Disk imaging — *See* disk cloning

Disk mirroring — A strategy whereby the same data is written to two hard drives in a computer, to safeguard against hard drive failure. Disk mirroring uses only a single adapter for two drives.

Disk striping — Treating multiple hard drives as a single volume. Data is written across the multiple drives in small segments, in order to increase performance and logical disk volume, and, when parity is also used, to provide fault tolerance. RAID 5 is disk striping with an additional drive for parity.

Dynamic drive — In Windows 2000, a hard drive that uses a 1-MB database written at the end of the drive to hold information about volumes on the drive and RAID setup information.

Encrypting virus — A type of virus that transforms itself into a nonreplicating program in order to avoid detection. It transforms itself back into a replicating program in order to spread.

Fault tolerance — The degree to which a system can tolerate failures. Adding redundant components, such as disk mirroring or disk duplexing, is a way to build in fault tolerance.

File virus — A virus that inserts virus code into an executable program and can spread whenever that program is accessed.

Full backup — A complete backup, whereby all of the files on the hard drive are backed up each time the backup procedure is performed. It is the safest backup method, but it takes the most time.

Incremental backup — A time-saving backup method that only backs up files changed or newly created since the last full *or* incremental backup. Multiple incremental backups might be required when recovering lost data.

Infestation — Any unwanted program that is transmitted to a computer without the user's knowledge and that is designed to do varying degrees of damage to data and software. There are a number of different types of infestations, including viruses, Trojan horses, worms, and time bombs, among others.

Macro — A small sequence of commands, contained within a document, that can be automatically executed when the document is loaded, or executed later by using a predetermined keystroke.

Macro virus — A virus that can hide in the macros of a document file. Typically, viruses do not reside in data or document files.

Material safety data sheet (MSDS) — A document that provides information about how to properly handle substances such as chemical solvents including physical data, toxicity, health effects, first aid, storage, disposal, and spill procedures.

Memory-resident virus — A virus that can stay lurking in memory, even after its host program is terminated.

Minicartridge — A tape drive cartridge that is only 3¼ × 2½ × ⅜ inches. It is small enough to allow two drives to fit into a standard 5½-inch drive bay of a PC case.

Multipartite virus — A combination of a boot sector virus and a file virus. It can hide in either type of program.

Non-memory-resident virus — A virus that is terminated when the host program is closed. Compare to memory-resident virus.

Polymorphic virus — A type of virus that changes its distinguishing characteristics as it replicates itself. Mutating in this way makes it more difficult for AV software to recognize the presence of the virus.

Quarter-Inch Committee or **quarter-inch cartridge (QIC)** — A name of a standardized method used to write data to tape. Backups made with the Windows 9x System Tools Backup utility have a .qic extension.

RAID (redundant array of inexpensive disks or **redundant array of independent disks)** — Several methods of configuring multiple hard drives to store data to increase logical volume size and improve performance, and to ensure that if one hard drive fails, the data is still available from another hard drive.

Retension — A tape maintenance procedure that fast-forwards and then rewinds the tape to eliminate loose spots on the tape.

Sequential access — A method of data access used by tape drives whereby data is written or read sequentially from the beginning to the end of the tape or until the desired data is found.

Spanned volumes — Windows 2000 method of linking several volumes across multiple hard drives into a single logical drive

Stealth virus — A virus that actively conceals itself by temporarily removing itself from an infected file that is about to be examined, and then hiding a copy of itself elsewhere on the drive.

Trojan horse — A type of infestation that hides or disguises itself as a useful program, yet is designed to cause damage at a later time.

Virus — A program that often has an incubation period, is infectious, and is intended to cause damage. A virus program might destroy data and programs or damage a disk drive's boot sector.

Virus signature — The distinguishing characteristics or patterns of a particular virus. Typically, AV signature updates for new viruses can be downloaded monthly from the Internet.

Volumes — In Windows 2000, a partition on a hard drive that is formatted as a dynamic drive.

Worm — An infestation designed to copy itself repeatedly to memory, on drive space, or on a network until little memory or disk space remains.

Review Questions

1. List one or two preventive maintenance measures that help protect each of the following: computer case, CMOS setup, floppy drive, hard drive, keyboard, mouse, printer, and software.
2. List three things that should be done before moving or shipping a computer.
3. How do you properly dispose of a battery pack from a notebook computer? A broken monitor? A toner cartridge from a laser printer?
4. List and describe three types of viruses.
5. List three ways to "catch" a virus.
6. List three ways to prevent a virus.
7. List three symptoms or problems that indicate that a virus might be present.
8. How is disk mirroring different from disk duplexing?
9. When one hard drive can be removed and another hard drive inserted without powering down a computer, this is called ________________.
10. Clearly explain how the child, parent, grandparent method works as a plan for reusing tapes.
11. How are differential backups different from full backups, and what are the advantages of each?
12. How are differential backups different from incremental backups, and what are the advantages of each?
13. Why would you want to "retension" a backup tape?
14. Give two reasons why you would want to schedule a hard drive backup to occur during the night.
15. Why is it important to verify that your disaster recovery plan works and to put it in writing?

Projects

Creating a Preventive Maintenance and Disaster Recovery Plan

Assume that you are a PC technician responsible for all of the 30 to 35 PCs of a small organization. The PCs are networked to a file server that is backed up each evening. No PC has power protection or line conditioning. Although some users make backups of data on their PC to tape drives or Zip drives, the company does not have a procedure to back up data or software. Your supervisor has asked you to submit a preventive maintenance and disaster recovery plan for these PCs and to estimate the amount of time you will spend each month for the next 12 months on preventive maintenance. She has also asked you to submit a suggested PC data backup plan for all users to follow, which will become a company policy. Do the following to create these plans and estimate your time.

1. List the possible causes of PC failures.

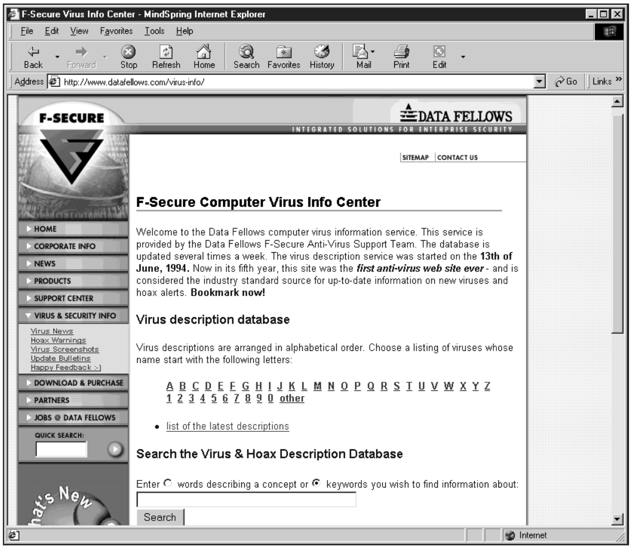
2. Using the list above, list what you can do to prevent these problems. Divide the list into two categories: what you plan to do one time for each PC or user, and what you plan to do on a routine or as-needed basis.
3. For each PC, estimate the amount of time you need to implement the one-time-only plan and the amount of time you need each year for ongoing maintenance.
4. Based on your answers to Question 3, how much time do you plan to spend, on average, each month for the next 12 months on preventive maintenance?
5. In response to the request for a recommended company policy to back up PC data, write a policy for users to follow to back up data on their PCs. Since all PCs are networked to the file server, suggest that company policy be that data on a PC should be backed up to the file server, where it will be backed up nightly in case of a file server failure. Write the backup policy and instructions on how to use it.

Hands-on Project

Using the Internet to Learn About Viruses

The classic source of information about viruses on the Web is Data Fellows. Go to the web site *www.datafellows.com/vir-info/*, shown in Figure 19-19, for information about viruses; the viruses are listed in alphabetical order with complete descriptions, including any known source of the virus. Print a description of three viruses from this web site:

1. One virus that destroys data on a hard drive
2. One harmless virus that only displays garbage on the screen
3. One virus that hides in a boot sector



Address: http://www.datafellows.com/virus-info/

F-Secure Computer Virus Info Center

Welcome to the Data Fellows computer virus information service. This service is provided by the Data Fellows F-Secure Anti-Virus Support Team. The database is updated several times a week. The virus description service was started on the **13th of June, 1994.** Now in its fifth year, this site was the ***first anti-virus web site ever*** - and is considered the industry standard source for up-to-date information on new viruses and hoax alerts. **Bookmark now!**

Virus description database

Virus descriptions are arranged in alphabetical order. Choose a listing of viruses whose name start with the following letters:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 0 other

- list of the latest descriptions

Search the Virus & Hoax Description Database

Enter ○ words describing a concept or ● keywords you wish to find information about:

Figure 19-19 For complete virus information, see the Data Fellows web site

Download the Latest Update of AV Software

If you own antivirus software, download the latest antivirus definition list from the Internet. For example, for Norton AntiVirus, follow these directions:

1. Log on to the AV site:

   www.symantec.com/avcenter

2. Click **Download Updates**. Answer the required questions, such as:

   Product: NAV for Windows 95

   Language: English, US

   Operating Environment: Windows 95

3. Follow the directions to download the latest update and signature list for the particular version of your AV software.
4. While online, see if the site offers information on virus hoaxes and create a list of hoaxes if it does.

Using Nuts & Bolts, McAfee VirusScan Software

Using the McAfee VirusScan software, scan a floppy disk for viruses.

Research the Market for a Tape Drive

To evaluate two tape drives for possible purchase, fill in the following table. Which drive seems more appropriate for a standalone PC that is used heavily for data entry and needs data backed up daily? Why?

	Tape Drive 1	Tape Drive 2
Product name		
Manufacturer		
Price		
Accelerator (yes/no/optional)		
Software included		
Type (internal/external)		
Warranty (1year/2 years/lifetime)		
Tape formats supported		
Maximum capacity (also indicate the tape format required to meet this maximum capacity, for example: 4.4 GB using QIC-3020)		
Types of cartridges supported		

Using Windows 98 to Back Up Files and Folders

This exercise lets you practice using Windows 98 Microsoft Backup and see how the Backup utility manages several situations.

Part I

1. Using Windows Explorer, create a folder called Backtest on a hard drive.
2. Use Explorer to find a .BAT file, and copy it to the new folder. Copy two other files to the Backtest folder. Make a subfolder called Subfolder in Backtest and copy a fourth file to C:\backtest\subfolder.
3. Right-click the .BAT file and rename it Overwrite.txt. Right-click the second file and rename it Delete.txt. Rename the third file NoChange.txt. The fourth file can be left alone for now. Use Explorer and write down the file sizes before the backup.
4. Click **Start**, **Programs**, **Accessories**, **System Tools**, and **Backup**.
5. Use the directions provided in this book to back up the folder Backtest to a floppy disk. Use Explorer and compare the backup file size to the original file sizes. How are they different?
6. Delete the file **Delete.txt**. Edit and change the contents of the file Overwrite.txt. Make no changes to the file NoChange.txt. Delete **Subfolder**.
7. Using Windows 98 Backup, restore the files from the backup to their original folder.
   a. What did Backup do with the Delete.txt file?
   b. What did Backup do with the Overwrite.txt file?
   c. What did Backup do with the NoChange.txt file?
   d. What did Backup do with the missing Subfolder and missing file?
   e. What is the name of the backup file on the floppy disk?
   f. What are the name and path to the error log created by Backup?
   g. Print the error log.

Part II

8. Use Windows Explorer to copy the Backtest folder to a second floppy disk.
9. Delete all the files in the Backtest folder on the hard drive.
10. Use Windows Explorer to copy the three files back to the Backtest folder.
11. Delete the files in the Backtest folder on the hard drive.
12. Open the Recycle Bin and restore the three files to the Backtest folder by highlighting the selected files and using the File, Restore option. Did they return to the correct folder?
13. Once again, delete the files in the Backtest folder on the hard drive.
14. Highlight the three files in the Recycle Bin, and choose **File**, **Delete**. Can you still restore the files?

Hands-on Project

Disposal Rules in Your Community

Research the laws and regulations in your community concerning the disposal of batteries and old computer parts. Answer these questions regarding your community:

1. How do you properly dispose of a monitor?
2. How do you properly dispose of a battery pack used by a notebook computer?
3. How do you properly dispose of a large box of assorted computer parts including hard drives, floppy drives, computer cases, and circuit boards?